IN THE UNITED STATES DISTRICT COURT
FOR NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF **ELECTRONIC DEVICES AND STORAGE MEDIA**, CURRENTLY LOCATED AT THE FBI BOSTON DIVISION EVIDENCE VAULT**, 201 MAPLE STREET, CHELSEA, MASSACHUSETTS, 02150-1821**	Case No. 23-mj-31-01-AJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH

I, **SSA Kathryn Thibault**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of properties—electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been employed with the FBI since 1998. I am currently assigned to FBI HQ Security Division, physically stationed to the FBI Knoxville Division in Tennessee. Prior to that, I was stationed in the Bedford, NH, office of the FBI Boston Division. While employed by the FBI, I have investigated federal criminal violations related to cyber-crime, child exploitation and child pornography. I have gained experience through training at the FBI Academy, field investigations and child exploitation training through various federal entities. I have observed and reviewed

numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

3. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched are the electronic devices and storage media listed below and in Attachment A, each of which was seized pursuant to a prior search warrant, [redacted] and are located at the FBI Boston Division Evidence Vault, 201 Maple Street, Chelsea, Massachusetts, 02150-1821:

a. White Samsung Cellphone, S/#: AA1DC13ZS/2-B, Model: SCH-1545V, Sim card intact, Micro SD card intact, SIM ID: TF256PSIMV9DD

b. One (1) Sony PlayStation black 8MB memory card, magic gate with the number SCPH-10020.

c. One (1) Sony Clear Memory Card number SCPH-1020.

d. One (1) ICY DOC computer doc container with RAM 14125365

e. One (1) black ICY DOC computer doc container with RAM 08524694.

f. One (1) Silver ICY DOC computer doc container with RAM 14129962.

g. Black and yellow ADATA UV 128/16 GB thumb drive.

h. One (1) Black Lenovo Thinkpad with various stickers on the exterior stating Bitcoin, LRN.FM, The Liberty Network and Free Talk LiveTalk Radio You Control. Serial Number: PC-00A7Y9. Battery removed.

i. One (1) NZXT Black computer tower with a swing open door. Inside the tower are eleven (11) slots for hard drives. Two Hard drives intact within the tower as well as RAM in the tower.

j. One (1) Leopard thumb drive with the Transformer Logo on it, 2GB storage.

k. One (1) black USB with a hole in the center of the USB.

l. One (1) Black USB with a chipped corner of the USB.

m. One (1) Black SanDisk Cruzer 8GB USB, white lettering on onside, not legible.

n. One (1) Corsair Flasher Survivor USB with the word STEALTH written on it, screw top type to hide the USB and contains 32 GBs of storage. USB has 3.0 written on it.

o. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E619566, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

p. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E617535, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

q. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E505658, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

r. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E588268, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

s. One (1) 150GB Hard Drive, serial number WXCOCA928644, Western Digital Velociraptor, enterprise storage with WD1500HLFS written on it.

t. One (1) 150GB Hard Drive, serial number WXD0CB971033, Western Digital Velociraptor, enterprise storage with WD1500HLFS written on it.

u. One (1) black pair of recording glasses.

v. One (1) Blue Transcend SD HC sim card in a clear plastic case.

w. One (1) Transcend lock Micro SD adapter with a 2GB Micro SD card in a plastic case.

x. One (1) Transcend lock Micro SD adapter with a 16GB Micro SD card in a plastic case

y. One (1) grey Canon HD Vixia HF100 Video Camera with a flip screen. SD card located inside camera slot for the video screen, unknown serial number.

z. CD case containing sixteen (16) CDs. CD's are marked with the following handwritten language to identify the disks: Music Beds 01:25 8/5/03, Music Beds 4xs Born 1:26 12/05/03; Cartoon Network Space Ghosts Musical Bar-B-Que, Cartoon Network Surf & Turf, Music A-S, Music S-Z, Music Beds Oroduction Stingers Production, Ultimate Boot CD, Office Professional 201, Win TV, PCI

Drivers, Win 7x64 Leave Serial Blank, Tails 2013-10-2, Win 7x64 SPI, Windows 10 Enterprise Privacy ED and MEMTEST 86.

aa. One (1) Western Digital Hard Drive bearing S/N: WMANT1137886 and WD Raptor, 36 GB.

bb. One (1) Seagate Barracuda Hard Drive bearing S/N: 3KB1KXNJ, Model: ST380023, 80 GB.

cc. One (1) grey HP Pavillion G Series Laptop, battery detached, SN: CNF1091WPK, Model:g4-1010us, with the stickers stating LRN.FM, The Liberty Radio Network and Free Talk Live Radio You Control.

dd. One (1) pair of black Durango Glacier recording sunglasses, SN: DU32271284

ee. One (1) Piratebox wifi emitter hotspot, 150mbps TL-MR3020, S/N: 12361601283, FCC ID: TE7MR3020.

ff. One (1) 32 GB Sandisk USB (Plugged into the Pirate Wifi Emitter listed above)

gg. Samsung Solid State Computer Drive (SSD) 840EVO, S/N: S1D5NSBF630248B, 120 GB, Model: MZ-7TE120.

hh. One (1) Silver external Hard Drive with a sticky note attached to it stating 'Vendor # FREE TALK", Label with "DJVCS", S/N: 6213TYX3TQQ7.

ii. One (1) OIRCO Leading Technology External Hard Drive, S/N: 110214E3834563GHRT9N, with the words "Easy your PC www.ORCO.COMCN" written on the drive.

jj. NZXT Desktop Computer Tower with a removable 16 GB Transcend SD HC SD card, no serial number because this is a personally built tower.

kk. Black case containing twenty-three (23) CD's labeled FTL Archive, Free Talk Live Season 1 "Real Radio" Disc 1 of 3; Free Talk Live Season 1 "Real Radio" Disc 2 of 3, Free Talk Live Season 1 Disc 3 of 3, Free Talk Live SeSON 1 "Real Radio" Disc 3 of 3; Free Talk Live Season 1 "Rental Radio" Disc 1 of 3 8/4/03 – 10/16/03 +: 60 Promos; Free Talk Live Season 1 "Rental Radio" Disc 2 of 3 10/20/03 – 01/09/04; Free Talk Live SeSON 1 "Rental Radio" Disc 3 of 3 1/12/04 – 9/11/04 and Seventeen (17) FTL GCN CD's marked with the dates of 2004-09-8/19 – 11/01/2015.

ll. Computer Tower with no name or serial number because hand constructed containing four (4) ICY DOC's with solid State Drives (SSD) inside the tower that has a keylock to open the computer tower.

mm. SafeNet Sentinel USB, labeled 204F, unknown GB aith an attached lable on the device marked "#204f dad", S/N: 0204F

nn. One (1) black Sansa Sandisk Media Player 2.0 GB

oo. One (1) black desktop ASUS, no serial number and no identifying features.

pp. One (1) Lenovo Ideapad 100 with a sticker stating Intel Core i3 inside, S/N PF0D2Z7S, Model Name: 80QQ, Windows type computer, FFC ID: TX2-RTL8723BE, various stickers on the xterior stating LRN.FM The Liberty Network, Shiresociety.com and Free Talk Live Radio You Control.

For purposes of this affidavit and warrant, I refer to these electronic devices and storage media collectively as the "Devices." The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

5. On March 18, 2016, United States Magistrate Daniel Lynch for the District of New Hampshire signed a federal search warrant authorizing the FBI to search the premises located at 73 and [redacted], New Hampshire (the "2016 Warrant"). I have attached and incorporate the 2016 Warrant as Exhibit A to this affidavit.

6. The 2016 Warrant authorized investigators to seize and search electronic devices found at the premises for evidence, contraband or fruits of violations of 18 U.S.C. § 2252(a)(4)(B), which criminalizes, among other things, the possession of child pornography. E.g., Ex. A at 42-43. The 2016 Warrant also authorized the seizure of property that was used or intended to be used to commit this criminal offense. Id.

7. As laid out in Exhibit A to this affidavit, there is probable cause that electronic devices found at the premises contain child pornography. Ex. A at 11-37.

8. On March 20, 2016, the FBI executed the 2016 Warrant and, pursuant to that warrant, seized the Devices and other electronic devices.

9. During and after the execution of the 2016 Warrant, the FBI searched and returned several electronic devices. Other devices—the Devices listed in paragraph four above—were seized but not fully searched at the time.

10. Pursuant to the 2016 Warrant, on March 20, 2016, FBI examiners conducted a preliminary search of two of the Devices—Leveno Laptop and the NZXT black computer tower and found what appeared to be child pornography.

11. The FBI did not fully search the Devices in 2016 primarily for two reasons. First, one of the Devices was encrypted and could not be fully searched by the local FBI forensic examiners. This required that Device to examined by another FBI forensic laboratory but the technology available at the time was unsuccessful in accessing the identified encrypted areas of the Device. Second, after the execution of the 2016 Warrant, the lead case agent transferred to a different location and the case was reassigned to me. I did not request a forensic examination of the other Devices seized from the scene after the case was reassigned.

12. When executing the 2016 Warrant, the FBI conducted an on-scene triage to make sure there was not any encryption other programs on the seized devices—including the Devices—that would alter or otherwise damage their data when FBI examiners later searched them. The Devices were collected and packaged per FBI policy and transported to the FBI Boston Division Evidence Vault. All seized devices—including the Devices—were secured within the evidence vault where no access is permitted without signing out the device. I have reviewed the evidence logs and none of the Devices were signed out from the evidence vault

except for 13 devices signed out by FBI forensic examiners in order to make forensic images to be reviewed.

13. I have conferred with two of the FBI forensic examiners who signed out the 13 devices and made the forensic images. They explained that these forensic images are identical copies of the data on the devices at the time the images were made and that the images were made without altering any of the data on the devices. This allows examiners to search the forensic image and so not risk modifying any data on the device itself.

14. Therefore, the Devices are in the same condition as when they were seized and, as laid out above and in Exhibit A, there is probable cause that they contain child pornography or are otherwise authorized to be searched pursuant to the 2016 Warrant.

15. The Devices are currently in the lawful possession of the FBI and are stored at the FBI Boston Division Evidence Vault.

16. Since the execution of the 2016 Warrant, on March 19, 2022, the owner of the Devices filed a civil suit seeking the return of the Devices. *Shire Free Church Monadnock and Ian Freeman v. Scott Bailey*, Docket No. 22-cv-00100-SM.

17. The FBI wishes to return the Devices but is concerned about returning them while there remains probable cause that they contain child pornography. The FBI offered to delete the content of the devices prior to returning them but the owner refused this offer. The owner also did not consent to the FBI searching the devices to confirm that they do not contain child pornography.

18. While the FBI may already have the necessary authority to examine the Devices under the 2016 Warrant, due to the passage of time, I sought and obtained a warrant on January 5, 2023 out of an abundance of caution to be certain that an examination of all the Devices will

comply with the Fourth Amendment and other applicable laws to allow the FBI to use advanced software techniques to locate any child pornography and related material on the Devices.

19. On January 5, 2023, Magistrate Judge Johnstone issued a warrant to search the Devices. 23-mj-1-01-AJ. On January 26, 2023, I submitted a ticket to the FBI forensic examiners to examine the Devices. Because I submitted a ticket after the 14 days required to execute the search warrant, I am seeking an additional warrant in an abundance of caution to ensure that any examination of the Devices will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of

four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

e. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

g. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

j. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

k. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

l. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

m. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

n. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. Because this warrant seeks only permission to examine the devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

/s/ Katheryn Thibault
Supervisory Special Agent Katheryn Thibault
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Date: Feb 22, 2023

Time: 12:03 PM, Feb 22, 2023

/s/ Andrea K. Johnstone
The Honorable Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

The property to be searched are the electronic devices and storage media listed below, each of which was seized pursuant to a prior search warrant, [redacted], and are located at the FBI Boston Division Evidence Vault, 201 Maple Street, Chelsea, Massachusetts, 02150-1821:

a. White Samsung Cellphone, S/#: AA1DC13ZS/2-B, Model: SCH-1545V, Sim card intact, Micro SD card intact, SIM ID: TF256PSIMV9DD

b. One (1) Sony PlayStation black 8MB memory card, magic gate with the number SCPH-10020.

c. One (1) Sony Clear Memory Card number SCPH-1020.

d. One (1) ICY DOC computer doc container with RAM 14125365

e. One (1) black ICY DOC computer doc container with RAM 08524694.

f. One (1) Silver ICY DOC computer doc container with RAM 14129962.

g. Black and yellow ADATA UV 128/16 GB thumb drive.

h. One (1) Black Lenovo Thinkpad with various stickers on the exterior stating Bitcoin, LRN.FM, The Liberty Network and Free Talk LiveTalk Radio You Control. Serial Number: PC-00A7Y9. Battery removed.

i. One (1) NZXT Black computer tower with a swing open door. Inside the tower are eleven (11) slots for hard drives. Two Hard drives intact within the tower as well as RAM in the tower.

j. One (1) Leopard thumb drive with the Transformer Logo on it, 2GB storage.

k. One (1) black USB with a hole in the center of the USB.

l. One (1) Black USB with a chipped corner of the USB.

m. One (1) Black SanDisk Cruzer 8GB USB, white lettering on onside, not legible.

n. One (1) Corsair Flasher Survivor USB with the word STEALTH written on it, screw top type to hide the USB and contains 32 GBs of storage. USB has 3.0 written on it.

o. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E619566, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

p. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E617535, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

q. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E505658, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

r. Western Digital Hard drive, 250 GB bearing serial number: WCAT1E588268, 16MB cache, WD Caviar Blue and WD2500AAKS written on it.

s. One (1) 150GB Hard Drive, serial number WXCOCA928644, Western Digital Velociraptor, enterprise storage with WD1500HLFS written on it.

t. One (1) 150GB Hard Drive, serial number WXD0CB971033, Western Digital Velociraptor, enterprise storage with WD1500HLFS written on it.

u. One (1) black pair of recording glasses.

v. One (1) Blue Transcend SD HC sim card in a clear plastic case.

w. One (1) Transcend lock Micro SD adapter with a 2GB Micro SD card in a plastic case.

x. One (1) Transcend lock Micro SD adapter with a 16GB Micro SD card in a plastic case

y. One (1) grey Canon HD Vixia HF100 Video Camera with a flip screen. SD card located inside camera slot for the video screen, unknown serial number.

z. CD case containing sixteen (16) CDs. CD's are marked with the following handwritten language to identify the disks: Music Beds 01:25 8/5/03, Music Beds 4xs Born 1:26 12/05/03; Cartoon Network Space Ghosts Musical Bar-B-Que, Cartoon Network Surf & Turf, Music A-S, Music S-Z, Music Beds Oroduction Stingers Production, Ultimate Boot CD, Office Professional 201, Win TV, PCI Drivers, Win 7x64 Leave Serial Blank, Tails 2013-10-2, Win 7x64 SPI, Windows 10 Enterprise Privacy ED and MEMTEST 86.

aa. One (1) Western Digital Hard Drive bearing S/N: WMANT1137886 and WD Raptor, 36 GB.

bb. One (1) Seagate Barracuda Hard Drive bearing S/N: 3KB1KXNJ, Model: ST380023, 80 GB.

cc. One (1) grey HP Pavillion G Series Laptop, battery detached, SN: CNF1091WPK, Model:g4-1010us, with the stickers stating LRN.FM, The Liberty Radio Network and Free Talk Live Radio You Control.

dd. One (1) pair of black Durango Glacier recording sunglasses, SN: DU32271284

ee. One (1) Piratebox wifi emitter hotspot, 150mbps TL-MR3020, S/N: 12361601283, FCC ID: TE7MR3020.

ff. One (1) 32 GB Sandisk USB (Plugged into the Pirate Wifi Emitter listed above)

gg. Samsung Solid State Computer Drive (SSD) 840EVO, S/N: S1D5NSBF630248B, 120 GB, Model: MZ-7TE120.

hh. One (1) Silver external Hard Drive with a sticky note attached to it stating 'Vendor # FREE TALK", Label with "DJVCS", S/N: 6213TYX3TQQ7.

ii. One (1) OIRCO Leading Technology External Hard Drive, S/N: 110214E3834563GHRT9N, with the words "Easy your PC www.ORCO.COMCN" written on the drive.

jj. NZXT Desktop Computer Tower with a removable 16 GB Transcend SD HC SD card, no serial number because this is a personally built tower.

kk. Black case containing twenty-three (23) CD's labeled FTL Archive, Free Talk Live Season 1 "Real Radio" Disc 1 of 3; Free Talk Live Season 1 "Real Radio" Disc 2 of 3, Free Talk Live Season 1 Disc 3 of 3, Free Talk Live SeSON 1 "Real Radio" Disc 3 of 3; Free Talk Live Season 1 "Rental Radio" Disc 1 of 3 8/4/03 – 10/16/03 +: 60 Promos; Free Talk Live Season 1 "Rental Radio" Disc 2 of 3 10/20/03 – 01/09/04; Free Talk Live SeSON 1 "Rental Radio" Disc 3 of 3 1/12/04 – 9/11/04 and Seventeen (17) FTL GCN CD's marked with the dates of 2004-09-8/19 – 11/01/2015.

ll. Computer Tower with no name or serial number because hand constructed containing four (4) ICY DOC's with solid State Drives (SSD) inside the tower that has a keylock to open the computer tower.

mm. SafeNet Sentinel USB, labeled 204F, unknown GB aith an attached lable on the device marked "#204f dad", S/N: 0204F

nn. One (1) black Sansa Sandisk Media Player 2.0 GB

oo. One (1) black desktop ASUS, no serial number and no identifying features.

pp. One (1) Lenovo Ideapad 100 with a sticker stating Intel Core i3 inside, S/N PF0D2Z7S, Model Name: 80QQ, Windows type computer, FFC ID: TX2-RTL8723BE, various stickers on the xterior stating LRN.FM The Liberty Network, Shiresociety.com and Free Talk Live Radio You Control.

For purposes of warrant, these electronic devices and storage media are referred to collectively as the "Devices." The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

ATTACHMENT B

All records on the Devices described in Attachment A that relate to violations of **Title 18, United States Code, Section 2252 (a)(4)(B)** including:

1. Records and information relating to the identity or location of the persons suspected of violating the statues described above;

2. Child pornography and child erotica;

3. Records and information relating to sexual exploitation of children;

4. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

5. Records evidencing the use of the Internet Protocol address [redacted] to communicate with **Website A** including:

   a. records of Internet Protocol addresses used;

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

   c. Evidence of software that would allow others to control the Devices, such as viruses, Trojan Horses and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software:

d. Evidence of the lack of such malicious software;

e. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.

f. Evidence indicating the computer user's state of mind as it related to the crime under investigation;

g. Evidence of attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

h. Evidence of counter-forensic programs and associated data that are designed to eliminate data from the computer;

i. Evidence of the times the computer was used;

j. Passwords, encryption keys and other access devices that may be necessary to access the computer; documentation and manuals that maybe necessary to access the computer to conduct a forensic examination of the computer;

k. Records of information about Internet Protocol addresses used by the computer;

l. Records of or information about the computers internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses;

m. Routers, modems and network equipment used to connect computers to the internet.

n. Child pornography and child erotica

o. Records, information and items relating to the occupancy or ownership of 73 Leverette Street, Keene, New Hampshire 03431 including utility and telephone bills, mail envelopes, or addressed correspondence; records, information and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access and handwritten notes;

p. Records and information relating to the identity or location of the persons suspected of violating the statues described above; and

q. Records and information relating to sexual exploitation of children, including correspondence and communications between users of Website A.

6. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures or photocopies).

7. The term "computer" includes all types of electronic, magnetic, optical, electrochemical or other high speed data processing devices performing logical, arithmetic or storage functions, including desktop computers, notebook computers. Mobil phones, tablets, server computers and network hardware.

8. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.